

Remarks / Arguments

The foregoing amendments and the following remarks are submitted in response to the Examiner's report of March 19, 2007. A response to the Examiner's report was due on June 19, 2007. The Applicants hereby request a one month extension of time for submitting the present response to the Examiner's report. The requisite fee of \$120 under 37 C.F.R. §1.17 (a)(1) is being submitted herewith. The Commissioner is hereby authorized to deduct any necessary fees from our deposit account number 12-2400 in this and future replies.

The Applicants thank the Examiner for her courtesy in agreeing to conduct a telephone interview with the Applicants' agent Fraser Rowand, on June 28, 2007. In the course of the interview, the Applicants' agent outlined the nature of the invention as described in the specification and as reflected in the claim limitations currently pending. The Examiner argued that the claim limitations may be found in the cited reference, U.S. patent number 5,768,381 to Hawthorne. The Applicants' agent noted that none of the elements described in Hawthorne, including the mutual primitive, the random session key, or the registered crypt string, act as a synchronization vector used to synchronize the encryption and decryption of data. Moreover, none of these elements, if considered a session key within the meaning of the claim language, result in Hawthorne's process fulfilling the claim limitations found in independent claim 1. In particular, Hawthorne's process does not show a step of creating a bitstream including a synchronization vector, generating an encryption signal based on a session key and encrypting the bitstream with the encryption signal, generating at a receiving set the encryption signal based on the session key and decrypting the encrypted bitstream using the encryption signal to identify the synchronization vector. In the course of the interview, the Examiner was unable to point to the specific elements within Hawthorne that met the limitations found in independent claim 1 of the present application. Nevertheless,

she was adamant that the claim was anticipated by Hawthorne. No agreement was reached between the Examiner and the Applicants' agent.

In order to assist the Examiner's understanding of the invention, the Applicants have amended independent claims 1, 8, and 15, as shown above. In particular, the Applicants have amended claim 1 to remove the "whereby" clause and introduce a step of synchronizing the encryption signal to the encrypted bitstream based on identification of the synchronization vector to permit recovery of the bitstream from the encrypted bitstream. Similar amendments have been made to independent claims 8 and 15. No new matter has been introduced by way of this amendment.

The present application relates to a method and system for synchronizing encryption and decryption in the context of streamed data. In certain applications, such as for example Voice-over-IP, fast real-time streaming of data is imperative to the proper functioning of the system and achievement of certain quality of service levels. Accordingly, when encrypting streamed data, the encryption and decryption process needs to be relatively fast without undue computational demands during the streaming process. One method for encrypting and decrypting streamed data in a relatively fast computationally simple manner is to create a pseudo-random bitstream at a transmitting end and combine the pseudo-random bitstream with the streamed data in a bitwise operation to create an encrypted bitstream. At a receiving end, the same pseudo-random bitstream is generated and is applied to the received encrypted bitstream in a reverse bitwise operation to recover the streamed data. Accordingly, it will be appreciated that it is necessary to generate the same pseudo-random bitstream at both the transmitting set and the receiving set. Moreover, it is necessary to apply the pseudo-random bitstream in a reverse operation at the receiving set at the exact same point in the encrypted bitstream at which the encryption first began. Accordingly, synchronization must be achieved.

The present invention uses this symmetric encryption-decryption mechanism of having the same pseudo-random bitstream used for encryption and decryption in transmitting and receiving sets, respectively. The pseudo-random bitstream is generated in each of the transmitting and receiving sets based upon a session key known to both sets. Using the same session key as an input to an encryption algorithm used by cryptographic engines (24, 34) in both the transmitting set and the receiving set results in generation of the same pseudo-random encryption signal in both sets.

In order to synchronize the decryption process with the onset of the encryption process, yet maintain a heightened level of security and render the encrypted signal more difficult to decipher, the present invention specifies that the bitstream containing the payload data include a synchronization vector derived from the session key. Both the transmitting set and receiving set are aware of the synchronization vector. In one embodiment, the synchronization may be the session key itself. The bitstream containing payload data and the synchronization vector is then encrypted by the pseudo-random streamed encryption signal to generate an encrypted bitstream. At the receiving set, the encrypted bitstream is received, the pseudo-random encryption signal is generated by a cryptographic engine (34), and it is applied to the received encrypted bitstream in a feedback cipher in an attempt to identify the synchronization vector. Once the synchronization vector is found, the receiving set knows that it has successfully synchronized the pseudo-random encryption signal to the encrypted bitstream and may let the decryption run, producing the decrypted payload data.

These aspects of the present invention are reflected in independent claim 1 of the

present application wherein a method is recited including a step of creating, at the transmitting set, a bitstream including a synchronization vector derived from a session key. Further steps of the method include generating, at the transmitting set, an encryption signal based upon the session key and encrypting the bitstream with the encryption signal. At the receiving set, the method includes generating the encryption signal (the same encryption signal as was generated at the transmitting set), decrypting the encrypted bitstream using the encryption signal to identify the synchronization vector, and synchronizing the encryption signal to the encrypted bitstream based on identification of the synchronization vector to permit recovery of the bitstream from the encrypted bitstream.

In her report of March 19, 2007, the Examiner rejected claims 1-7, 8-14, 15-21, 22-23, and 25-32 under 35 U.S.C 102 (b) as being anticipated by Hawthorne. Claims 24, 33, and 34 were rejected under 35 U.S.C 103 (a) as being obvious having regard to Hawthorne in view of an excerpt by Menezes (Handbook of applied cryptography). For the reasons given below, the Applicants respectfully traverse the Examiner's rejection and submit that the claims of the present application, as amended, are both novel and non-obvious over the cited references.

In her rejection of March 19, 2007, the Examiner refers to column 5, lines 45-49 of Hawthorne as evidence that Hawthorne includes a creating a bitstream including a synchronization vector derived from a session key. This portion of Hawthorne describes the encryption of his main message using a random session key. It was not clear to the Applicants which element of Hawthorne was considered to be the synchronization vector and/or session key. During the telephone interview with the Applicants' agent, the Examiner was unclear on which element of Hawthorne she considered to be the synchronization vector and/or session key. After originally suggesting it was the random session key, she retracted that position and suggested

it may have been the mutual primitive or the registered crypt string. Because the Examiner has not been able to identify the exact basis for her rejections, the Applicants are put in the position of refuting each of these possibilities and demonstrating that Hawthorne fails to satisfy the claim limitations irrespective of which of these elements is considered to be the session key or synchronization vector recited in the claim language. Each possibility is considered below.

1. Random session key is the synchronization vector

The first possibility considered is that Hawthorne's "random session key" constitutes the synchronization vector recited in claim 1 of the present application. As indicated in claim 1, the synchronization vector is derived from a session key. In some embodiments, the synchronization vector may be the session key. The first step of the method recited in claim 1 is creating a bitstream including a synchronization vector derived from a session key. Hawthorne describes transmission of a "main message" from a transmitting set to a receiving set. Hawthorne teaches that the main message is first encrypted by the random session key (column 5, lines 45-49) to form an encrypted main message. The random session key is then encrypted by the mutual primitive to form an encrypted session key (column 5, lines 50-52). The encrypted session key is then attached as a header to the encrypted main message (column 5, lines 52-55). Accordingly, Hawthorne teaches the encryption of a main message by the random session key, the encryption of the session key by the mutual primitive, and the attachment of the encrypted session key as a header to the encrypted main message. If we assume the random session key in Hawthorne is the "synchronization vector" recited in claim 1, then the attachment of the encrypted session key to the encrypted main message might be interpreted as a step of "creating a bitstream including a synchronization vector".

Claim 1 then recites a step of generating an encryption signal based upon the session key and encrypting the bitstream with the encryption signal. Such a step would require that the "bitstream", i.e. the random session key (already encrypted) together with the main message (already encrypted), be further encrypted by an encryption signal generated based on the random session key. No such step appears in Hawthorne.

If instead, one considers the bitstream to constitute the random session key alone (without the main message) then claim 1 provides that the bitstream is to be encrypted by an encryption signal generated based on the session key. The synchronization vector is also derived from the session key. Accordingly, to meet this claim limitation Hawthorne's random session key (the bitstream) is to be encrypted by an encryption signal generated based on the random session key. Hawthorne contains no such teaching. In Hawthorne, the random session key is encrypted by the mutual primitive. The mutual primitive is wholly unrelated to the random session key and cannot be said to be an encryption signal generated based on the random session key. Therefore, Hawthorne fails to teach this aspect of claim 1.

Finally, Hawthorne contains no step of synchronizing an encryption signal to an encrypted bitstream at a receiving set based on identification of the random session key, since Hawthorne does not relate to encryption and decryption of streamed data using a pseudo-random bitstream. Accordingly, the issue of synchronization does not arise for Hawthorne.

2. Mutual primitive is the synchronization vector

The mutual primitive is an encryption key developed at the sending device (61) and transmitted to the receiving device in encrypted form (62) as a transfer key encrypted using a one time key during a key management setup process. At the receiving device, the transfer key is decoded and the mutual primitive is recovered. The mutual primitive is then encrypted using a unique pseudo-random code known only to the receiving device. This results in the registered crypt string. The registered crypt string is returned to the sending device where it is stored for use in subsequent communications.

On sending a message from a transmitting device to a receiving device in Hawthorne, the transmitting device encrypts a main message with a random session key (unrelated to any of the other keys). As a header to the encrypted main message, the sending device attaches the random session key encrypted by the mutual primitive (which the transmitting device is capable of recreating as needed). It also attaches the registered crypt string as a header. Accordingly, the receiving device receives a main message encrypted by the random session key, the random session key encrypted by the mutual primitive, and the registered crypt string. On receipt of this package, the receiving device is capable of decoding the registered crypt string (74) using the pseudo-random encryption key known only to the receiving device in order to recover the mutual primitive. It may then use the mutual primitive to decrypt the encrypted session key and recover the random session key. Now that the receiving device is in possession of the random session key, it can decrypt the main message.

It will be appreciated that the message sent from a transmitting device to the

receiving device includes an encrypted main message, an encrypted session key, and the registered crypt string. It does not include the mutual primitive. Accordingly, there is no step of creating a bitstream at the transmitting set where the bitstream includes a synchronization vector if the synchronization vector is considered to be the mutual primitive in Hawthorne.

The mutual primitive is present within the registered crypt string, since the registered crypt string is the mutual primitive encrypted by the pseudo-random encryption key generated at the receiving set. However, there is no step in which this pseudo-random encryption key is generated at the transmitting set, as required by claim 1. Therefore, if the mutual primitive taught in Hawthorne is considered to be the synchronization vector, Hawthorne fails to teach or suggest all of the steps recited in claim 1.

3. Registered crypt string is the synchronization vector

If Hawthorne is interpreted such that the registered crypt string is considered the synchronization vector recited in claim 1, one must interpret the "bitstream" as being the registered crypt string itself or the registered crypt string together with the encrypted main message. In either case, there is no step of generating an encryption signal based upon a session key and encrypting such a bitstream with the encryption signal. The registered crypt string is, at no point, encrypted by an encryption signal. Accordingly, Hawthorne fails to teach or suggest the steps recited in claim 1.

Summary

As set out above, irrespective of which element of Hawthorne one considers to be a synchronization vector within the meaning of claim 1, the remainder of Hawthorne's teachings do not fit with the claim language of the present application. Hawthorne teaches a complicated key management process inapplicable to the present application. The method recited in claim 1 includes embedding a synchronization vector derived from a session key in a bitstream, generating an encryption signal based on the session key, and encrypting the bitstream with the encryption signal. No such process is taught in Hawthorne. Moreover, one would not be inclined to modify the teachings of Hawthorne to arrive at such a process; since Hawthorne does not wish to provide for reversible stream ciphering, as indicated in column 4, lines 39-54. Accordingly, the Applicants respectively submit that claim 1 of the present application is both novel and non-obvious over Hawthorne.

Independent claims 8 and 15 contain similar limitations to claim 1 and the Applicants respectively submit that these claims are also novel and non-obvious over Hawthorne for the same reasons set out above, as are dependent claims 2-7, 9-14, and 16-21.

The excerpt from Menezes was cited by the Examiner on the basis that it teaches a step of receiving an index from a call centre. Accordingly, the Menezes reference does not assist in curing the deficiencies of Hawthorne in relation to the limitations of independent claims 1, 8, and 15. Therefore, the Applicants respectively submit that the pending claims are non-obvious over the combination of Hawthorne and Menezes.

Reconsideration and withdrawal of the Examiner's rejections under 35 U.S.C 102 (b) and 35 U.S.C 103 (a) is respectively requested.

Should the Examiner' be inclined to maintain her rejections based on Hawthorne, the Applicants would appreciate receiving a detailed explanation of the basis for the rejection including identification where the claim limitations of the present application may be found in the Hawthorne reference. If the Examiner would like to discuss the foregoing amendments or arguments, she is invited to contact the Applicants' agent Fraser Rowand, at 416-868-1482.

Respectfully Submitted,
Nortel Networks Limited

By: 

Fraser D. Rowand, Reg'n. No. 53,870

Place: Toronto, Ontario, Canada
Date: July 6, 2007
Tele No.: 416-868-1482